Headquarters
Eighth United States Army
Installation Management Command
Korea

Army in Korea
Supplement 1 to AR 25-1

2 July 2009

Information Management

ARMY KNOWLEDGE MANAGEMENT AND INFORMATION TECHNOLOGY

FOR THE COMMANDING GENERAL:

LEWIS F. SETLIFF III
Colonel, GS
Chief of Staff

Official:

GARRIE BARNES
Chief, Publications and
Records Management

Summary. This supplement prescribes policies and assigns responsibilities for Army Knowledge Management and Information Technology Management for the Army in Korea (AK).

Summary of change.

- o Corrects typographical and grammatical errors throughout the publication.
- o Corrects broken hyperlinks throughout the publication.
- o Corrects paragraph numbering to match up with the revised AR 25-1 dated Dec 2008.
- o Updates name change of RCIO-K to CESO-K throughout the supplement.
- o Revised the e-mail naming chart

Applicability. This supplement applies to all Army organizations in Korea and all DOD or non-DOD organizations using AK networks.

Supplementation. Organizations will not supplement this supplement without Communications Enterprise Services Office, Republic of Korea Region, (CESO-K) approval.

Forms. Army in Korea (AK) forms are available at http://8tharmy.korea.army.mil/g1_ag/.

Records Management. Records created as a result of processes prescribed by this supplement must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System (ARIMS) Web site at https://www.arims.army.mil

Suggested Improvements. The proponent of this supplement is CESO-K. Users may suggest improvements to this supplement by sending an e-mail to cesokpubs@korea.army.mil.

Distribution. Electronic Media Only (EMO).

AR 25-1, 4 December, 2008, is supplemented as follows:

Paragraph 2-16g, Army Service Component Commanders. Add the following:
Within Eighth Army, the command records administrator is the Chief, Publications and Records Management, Assistant Chief of Staff G1, OSD (G1).

Paragraph 2-24, Commanders or directors of major subordinate commands , field- operating agencies, separately authorized activities, tenant, and satellite organizations. Add subparagraphs c through f:

c. Commanders of Eighth Army major subordinate commands (AK Regulation 10-5, Appendix A) will ensure their organizations comply with the processes outlined in this supplement.

d. Information Management Officers (IMOs) are primarily responsible for initial triage and problem resolution. For maintenance assistance beyond the IMO's capability, the IMO should contact the Korea Theater Support Center (KTSC) Help Desk by dialing TECH (8324).

e. All units and activities will certify annually (NLT 31 JUL) that all IT hardware resources are recorded and 100 percent accurate in the Federal Information Processing System (FIPS) Management System (FMS).

f. The 1st Signal Brigade has the sole contracting responsibility for all local commercial telecommunications requirements with local vendors.

Paragraph 2-28, Communications Enterprise Services Office, Republic of Korea Region, (CESO-K) Responsibilities. Add paragraph 2-28:

a. CESO-K operates under the technical control (TECHCON) of NETCOM ESTA, the operational control (OPCON) of Installation Management Command Korea Region (IMCOM K), and the administrative control (ADCON) of 1st Signal Brigade.

b. CESO-K exercises TECHCON over the AK Directors of Information Management (DOIMs).

c. For AK, CESO-K executes and enforces common-user IT policies, standards, architectures, programs, and plans, while championing IT resource requirements and influencing IT decisions.

Paragraph 2-29, Other Army in Korea (AK) Responsibilities. Add paragraph 2-29:

a. Eighth Army CIO/ACofS G6. Eighth Army CIO/ACofS G6 is the approval authority for:

(1) Defense Red Switch Network telephones / Voice Over Secure Internet Protocol (VoSIP).

(2) Official DSN and asymmetric digital subscriber line (ADSL) lines in the quarters of preferred subscriber service (PSS) customers according to paragraph 6-4g. To be considered for this service, customers must be listed on the USFK J1 Key Billet List. Class-B DSN service is not permitted in quarters.

(3) Exceptions to policy to this supplement. Otherwise, Eighth Army CIO/G6 ensures all AK organizations follow the procedures outlined in this regulation and supplement.

b. HQ Eighth Army Staff Principals. Each HQ Eighth Army staff principal will:

(1) Designate a primary and alternate Information Management Officer (IMO), a primary and

alternate information assurance security officer (IASO), and a primary and alternate telephone control officer (TCO) for its staff office.

(2) Coordinate the fielding of new information systems (ISs) with Eighth Army CIO/ACofS G6 prior to fielding. This applies to AK-initiated IS fielding's and those directed by higher headquarters. Each staff principle must:

(a) Provide early and continuing notification to Eighth Army CIO/G6 of proposed IS fielding's.

(b) Obtain Defense Information Technology Security Certification and Accreditation Process (DIACAP) accreditation.

(c) Obtain Networthiness certification.

(3) Comply with the policies and procedures outlined in this supplement.

c. Staff Judge Advocate (SJA), Eighth Army. In addition to the responsibilities in subparagraph 2.a above, Eighth Army SJA will evaluate the legal aspects of requests for commercial network services at government expense in the quarters of key billet AK personnel.

Paragraph 3-2, Information management organizations below Headquarters, Department of the Army. Replace subparagraph f and add subparagraph g:

f. Other Army in Korea Tenant and satellite organizations, separately authorized activities, government-owned / contractor-operated facilities, regional support activities, U. S. Army Reserve regional readiness commands, field operating agencies (FOAs), and major staff entities will designate:

(1) A primary and alternate Information Management Officer (IMO), with the primary IMO in the minimum grade level of E-6 or civilian equivalent GS / KGS 7 or above. IMO appointment orders will be signed by an O-5 or GS equivalent within the organizations chain of command. IMOs must meet investigative levels as detailed in Table 4-3 of AR 25-2 and complete IMO certification training within 60 days of appointment. (Contact local Area DOIM for schedule.) The IMO is the commander's primary staff representative for IT/IM issues. The IMO will identify his/her organization's information requirements to the supporting DOIM. Each organization will coordinate with its Area DOIM for service level agreements. Each organization will identify an IMO to the next higher headquarters. Each major subordinate command (MSC) and Eighth Army staff section will submit an IMO appointment memorandum to its Area DOIM for processing. Each IMO will maintain a copy of his/her current IMO appointment memorandum. The IMO's responsibilities encompass the IM/IT areas of: communications systems and system support, visual information, information assurance, and automation. The IMO's core duties include, but are not limited to:

(a) Provide business management oversight, advice, and coordination of all IM/IT functions for the organization.

(b) Act as liaison between the organization and the local DOIM to obtain common-user C4/IT services from the DOIM.

(c) Assist the commander in exercising responsibility to effectively manage business processes associated with IM/IT assets in support of the organization's mission.

(d) Coordinate and monitor all common-user C4/IT baseline service and above baseline service with the DOIM.

(e) Identify and validate requirements and funding for above baseline services.

(f) Comply with Information Assurance requirements in AR 25-2 and AK Supp 25-2.

(g) Develop, establish, implement, and enforce organizational IM/IT policies and procedures.

(h) Manage the content and oversee the development and security of organizational automated applications.

(i) Develop and maintain the organization's Information Resource Management Program (IRMP). This includes life-cycle replacement of automation and required software upgrades to comply with Army Enterprise Licensing and security requirements.

(j) Manage and validate the organization's Requirement Documents.

(k) Manage Automation Asset Redistribution, Frequency Management, Terminal Services Access Controller System (TSACS), Federal Information Processing System (FIPS) program and Software Management.

(l) Review and provide input to the Army IT Metrics Program per instructions in DA Pamphlet 25-1-1, para. 6-5b(2)(d).

(m) Act as the organization's first-line POC for the triage of IT equipment, software, or process failures.

(n) Ensure system and user compliance with theater-level Enterprise Management requirements and procedures.

(2) A primary and alternate Information Assurance Security Officer (IASO). IASO duties and responsibilities are identified in AR 25-2 and AK supp 25-2 "Information Assurance."

(3) A primary and alternate Telephone Control Officer (TCO). TCOs must complete TCO certification training within 60 days of appointment. (Contact local Area DOIM for schedule.) The TCO is the commander's primary staff representative for telephone issues. The TCO will identify their organization's telephone requirements to the supporting DOIM. Each organization will coordinate with its Area DOIM for service level agreements. Each organization will identify a TCO to the next higher headquarters. Each major subordinate command (MSC) and Eighth Army staff section will submit a TCO appointment memorandum to its Area DOIM for processing. Each TCO will maintain a copy of their current TCO appointment memorandum.

g. 1st SIG BDE serves as the approval authority for all service level agreements (SLAs).

Paragraph 3-3a, Information management/information technology resource management. Add subparagraphs (8) through (11):

(8) C4/IT Initiatives:

(a) Communications Enterprise Services Office, Republic of Korea Region (CESO-K), will:

(i) Oversee and review unique office automation initiatives that are not C2.

(ii) Validate ongoing office automation projects via the Requirement Document process.

(iii) Change office automation project priorities as necessary.

(b) Eighth Army CIO/ACofS G6, in conjunction with Eighth Army ACofS G3, will:

(i) Oversee and review unique tactical and strategic C2 and C4/IT initiatives.

(ii) Validate all ongoing tactical C4/IT system projects via the operational needs statement (ONS) process.

(iii) Change all tactical C4/IT project priorities as necessary.

(9) All AK C4/IT special initiatives require Eighth Army CIO/ACofS G6 approval.

(10) The AK Configuration Control Board (CCB) will evaluate and recommend to the Eighth Army CIO/ ACofS G6 the prioritized IT requirements for AK. The CCB is responsible for establishing and maintaining the AK overall IT portfolio. The CCB will meet at least once a quarter or more often if necessary.

(11) Each Configuration Control Board (CCB) member will work with his or her local C4/IT senior managers to conduct a mission analysis before attending CCB meetings. Mission analysis is a strong, forward-looking, and continuous analytical activity that evaluates the ability of the organization's assets to meet existing and emerging demands for services. Mission analysis enables the organization to determine and prioritize the most critical capability shortfalls and best technology opportunities for improving overall security, capacity, efficiency, and effectiveness in providing services to customers.

Paragraph 3-3d, Budgeting and Execution of C4/IT Investments. Add subparagraphs (5) through (8):

(5) AK organizations and HQ Eighth Army staff offices will comply with the policies and procedures on C4/IT acquisition outlined in this supplement.

(6) All IT items must have an approved Requirement Document (RD) before they are procured unless they are identified on the DOIMs' RD exemption lists. Some items may be procured without an RD and without DOIM approval. Some items may be procured without an RD, but still require DOIM approval.

RD Exemption List without DOIM Approval: https://www.us.army.mil/suite/doc/15713064

RD Exemption List with DOIM Approval: https://www.us.army.mil/suite/doc/15713065

The unit making the request must send the Requirement Document to the local DOIM's office for validation and processing. RD Instructions: https://www.us.army.mil/suite/doc/8425124.

(a) All information communications technology (ICT) equipment purchases/leases that meet any of the following conditions for Modified Table of Organization and Equipment (MTOE) units must be approved by HQDA ACofS G3. Refer to AR 71-9 "Materiel Requirements" for further guidance.

(i) Any item or system that exceeds the Other Procurement, Army (OPA) threshold of $250,000.

(ii) Any item that is to be procured under an existing Army program using Other

Procurement, Army (OPA) dollars.

(iii) Any L-, KU-, or Tri-band commercial satellite system or service.

(iv) Command, control, communications, and computers (C4) data package assemblies containing commercial multiplexers, routers, data switches, voice switches, cryptographic equipment, modems, packet accelerators, and similar ancillary devices.

(v) Information assurance / computer network defense hardware and software (e.g., firewalls, intrusion detection systems, etc.). See 011601Z FEB 05 message from DA Washington, subject: Operational Purchases…for all MTOE Units.

(vi) Unit Operations Centers (UOCs) that employ Voice over Internet Protocol (VoIP) technology on classified and unclassified Intranets.

(vii) Tactical Operations Centers (TOCs) that include C4/IT equipment (e.g., large screen displays, servers, routers, fiber or wireless networks, very small aperture satellite terminals, etc.).

(viii) Single-/Multi-channel radio sets employed in combat, combat support, and combat service support tactical operations (i.e., UHF FM, VHF FM, HF AM, Tactical satellite, and squad radios). Note: Non-secure exception of the ICOM F40/43 handheld squad radio previously validated by HQDA ACofS G3.

(ix) Any radio system other than joint tactical radio system (JTRS) to include those systems operating above 2 GHz. This is IAW DOD policies "Radio Acquisitions" dated 28 AUG 1998 and "Radio Frequency (RF) Equipment Acquisitions Policy" dated 17 JUN 2003.

(x) Any wireless devices, services, and technologies that are integrated or connected to DOD networks must comply with DOD Directive 8500.1 and DOD instruction 8500.2. For further guidance, see DOD Policy "Use of Commercial Wireless Devices, Services, and Technologies in the DOD Global Information Grid (GIG)" dated 14 APR 2004.

(xi) Any item that does not have an associated and specified means of encryption.

(xii) Any RF emitting device that has a specific purpose supporting United States and Possessions (US&P) garrison and movement operations.

(xiii) Any IT support item that requires commercial and/or civilian contractual support (airtime, maintenance, etc.).

(b) Items for MTOE units that do not require HQDA ACofS G3 approval include:

(i) Replacement of components of items, assemblies, and systems that were previously authorized under the AR 71-9 approval process. This includes non-repairable and obsolete components.

(ii) Items to support DOIM installation IT or base operations (BASOPS) support using authorized funding.

(iii) LAN components.

(c) Additional requirements:

(i) Organizations requiring communications equipment not currently authorized by the MTOE will submit an operational needs statement (ONS) to the HQDA ACofS G3, IAW AR 71-9.

(ii) Organizations requiring satellite communications equipment must also begin the process with an operational needs statement (ONS), identifying their specific requirements to be submitted to DA for approval prior to any acquisition.

(7) Only an Information Management Officer (IMO) with valid appointment orders on file with the DOIM may request IT hardware or software. Personnel who attempt to order IT hardware or software without having an appointment letter on file will have their request returned without action. It is the responsibility of each organization's commander (or equivalent) to ensure current letters of appointment are filed with the local DOIM.

(8) Inventory Reporting. Federal Information Processing System (FIPS) Management System (FMS) is the principal repository of all Eighth Army automation equipment data. All AK organizations' IMOs will certify annually with CESO-K that their FMS data is 100 percent accurate. IMOs will submit an "Annual FMS Certification Memorandum," located at https://www.us.army.mil/suite/doc/12988279, NLT 31 JUL each year.

Paragraph 3-5, Process analysis and business/functional process improvement. Add subparagraph g.

g. AK organizations considering significant IT investments should contact Eighth Army CIO/ACofS G6 for information and assistance on process analysis and improvement.

Paragraph 3-6, Chief Information Officer validation of requirements. Add subparagraph c:

c. Eighth Army CIO/ACofS G6 validates technical solutions costing greater than $25K for **tactical** C4/IT requirements in the AK. CESO-K validates technical solutions costing greater than $25K for all other AK C4/IT requirements. Validation criteria include:

(1) A statement that all materiel solutions must be Joint Technical Architecture—Army (JTA-A) compliant.

(2) Evaluation of emerging technologies.

(3) Outcome-oriented performance measurements.

(4) Compliance with IA requirements.

(5) Evaluation of new or modified requirements against existing systems.

(6) 3-year life cycle replacement schedule.

(7) Compliance with the policies and procedures outlined in this supplement.

Paragraph 3-7, Information technology performance measurements. Add subparagraphs k and l:

k. Quantity Determination. Quarterly AK installation, the supporting signal battalion and area support activity (ASA) commander must collect, compile, and report the data necessary to build the overall evaluation for each IT metric (command, control, communications, computers, intelligence, surveillance, and

reconnaissance (C4ISR) capabilities documented in common levels of service) reported to Eighth Army and HQDA. The signal battalion and ASA IT metric managers (and their respective commanders) will determine the required quantity of each IT metric that is required for the installation to fully accomplish its power-projection, sustainment, or training mission at 100 percent. This requirement is called "full mission requirement." (Tactical C4ISR capabilities are not measured or reported by this process.)

(1) The ratio of "current capabilities" to the "full mission requirement" results in a percentage rating for that particular IT metric. Weights and standards for individual installation metrics and attributes are set by the Eighth Army CIO to adjust for their relative importance in meeting the IT support mission of an installation.

(2) The weight factors assigned to each metric allow their weighted scores to be rolled up into a "percentage" rating for each attribute reported. Similar weight factors allow "attributes" to roll up into a percentage rating for the IT "capability."

(3) Compiled IT metrics data will be used to identify mission-capability shortfalls and determine the budgetary requirements and the allocation and utilization of available IT resources.

(4) The AK IT metrics POC at CESO-K will validate IT metrics data submitted by the signal battalions and area support activities (ASAs) and send the information to HQDA quarterly.

l. Collection Process. The Army IT Metrics Process uses a single collection process to fulfill two HQDA-level reporting requirements. The metrics collected serve both the Army IT Metrics Program and the Army Installation Status Report (ISR) Program. Individual Area DOIMs collect the metrics data and report it to CESO-K. Using standards and weights provided by HQDA, centralized software analyzes the consolidated results and produces two key reports for each installation. One of the key reports is the IT Metrics Report and the other key report is the calculated scoring for the IT portion of ISR Part III based upon the IT Metrics results. The scoring for Part III of the ISR contains each installation's "color" ratings, ready for inclusion in the DOIM report to the ISR POC at each installation. The Area DOIMs can then use the ISR "color" ratings to prepare their Part Ill inputs to the consolidated theater-level ISR.

(1) The collection and reporting cycle for IT Metrics and ISR is quarterly.

(2) Each Area DOIM will ensure IT Metrics data is collected and reported to the IT Metrics Program. Function as the IT Metrics Focal Point for Area installations; grant "write" access to approved installation-level data entry personnel; submit installation IT Metrics data to CESO-K for validation; ensure ISR Part III Report is produced and presented to installation ISR Part III POC; and keep identification and contact information current in the DA CIO/ACofS G6 IT Metrics POC Web site.

(3) Area Support Activity Information Management Officers (IMOs) and tenant activity IMOs will ensure IT Metrics data they are responsible for collecting is reported to their supporting Area DOIM.

(4) CESO-K will ensure IT Metrics data is collected and reported to the IT Metrics Program; function as the IT Metrics focal point for AK; validate Area DOIM submissions and forward to HQDA for review; brief ISR Part III, Services 15, 16, 18 and 19, to Director, Installation Management Command Korea (IMCOM Korea); keep identification and contact information current at the DA CIO/ACofS G6 IT Metrics POC Web site; and establish quarterly collection procedures for the IT Metrics program within Korea.

Paragraph 3-8, Information technology/National Security System acquisition process. Add subparagraphs g.

g. Requirement Document. In the AK, the capability document per AR 71-9 is referred to as the Requirement Document, hereafter, designated as RD. The RD is used to request authorization to purchase

most IT hardware, software, services or a combination. In the AK, the CESO-K is the final approval authority for these documents. (See paragraph 3-3d(6).).

(1) The IMO must validate and an O-5 or above commander (or GS-14 or above director) must sign all RDs for IT requirements prior to submission to the Area DOIM.

(2) The Area DOIM shall process all requirement documents; provide a technical solution that is in compliance with the Army Enterprise Architecture, and forward recommendations through the Regional DOIM to CESO-K for final review/disposition. For RDs returned to the organization without action by the Area DOIM, sufficient justification must be provided.

(a) When a technical solution costs $25K or more, the Area DOIM will make recommendations via the Regional DOIM to CESO-K and DA CIO/ACofS G6, as appropriate. In either case, the IMO will receive approval/disapproval notice directly from their Area DOIM.

(b) Splitting IT requirements into multiple purchases to circumvent the $25K approval process is prohibited. Also AK organizations will not split IT requirements to circumvent the need to obtain a DA CIO/ACofS G6 waiver when using non-IT programmed funds for expenditures that exceed $25K (OMA).

(c) The Area DOIMs will forward all approved IT acquisition Requirement Documents, along with their technical solutions, to CESO-K for final approval.

(d) Life cycle replacements: For computers, monitors, printers, and other IT FMS reportable products, a list of excess items (targeted for turn-in to DRMO) must accompany the RD in one of the formats identified in paragraph 17c, AK Pam 25-1.

(e) Approved waivers if appropriate. Waivers are required for the following circumstances:

(i) A PM CHESS waiver is required when IT hardware costs $25K or more and the products are not currently available on an existing Army/DoD Enterprise Agreement or from CHESS managed contracts. This cost is IT equipment only. It does not include materials required to complete an installation such as cabling, Panduit labor, etc.

(ii) A PM CHESS waiver is required when a technical solution is provided for Commercial Off-The-Shelf software products (any price) and not included in an Enterprise Software Agreement.

(iii) A DA CIO/ACofS G6 waiver is required for using non-IT programmed funds (OMA) and the technical solution over $25K or more.

(f) Consolidated Buy (CB) Program. For the procurement of desktop and notebook computers and monitors, DA CIO/ACofS G6 policy requires purchase from the CHESS CB Program regardless of dollar value. AK organizations shall use the CB to satisfy their desktop and notebook requirements to the maximum extent possible. The CHESS currently conducts consolidated computer buys in February/March and August/September each fiscal year. AK organizations are reminded to coordinate their desktop and notebook acquisition requirements through their local Area DOIM. Exceptions to the CB can be granted by the CESO-K under the following criteria: Mission critical requirements, non-CB configuration requirements, and mandatory OCONUS host-country agreements. The specific exception must be adequately justified in the RD.

(g) In accordance with paragraph 12, USFK Regulation 715-2, all IT acquisition purchase requests (PR) must have an approved RD attached to the PR IAW with USACCK Instructions for Aquiline PR Web Purchase Request.

(3) All IM and IT acquisitions of requirements costing $3,000 or less (except those noted in the subparagraph below) must be procured with a Government Purchase Card (GPC). Other uses of the GPC for IM or IT items are prohibited. IT acquisitions exceeding $3,000 must be procured through U.S. Army Contracting Command, Korea (USACCK) via the Purchase Request Web (PRWeb) process. Splitting IT requirements into multiple purchases to circumvent the $3,000 GPC single-purchase limit is prohibited. Warranty and maintenance for items purchased from an open market source is the responsibility of the user.

(a) Cell Phones: All cell phones must be procured from the AK cell phone contract (https://www.us.army.mil/suite/doc/15711272) through the RD process. Each cell phone RD must identify quantities of the following items: tier (1 or 2), period of use (full time or exercise), & monthly service plan (number of minutes). Each cell phone RD must also identify the requiring organization's Commander, Ordering Officer (GPC Holder), Telephone Control Officer (TCO), & Delivery POC. An example of a cell phone RD is located at https://www.us.army.mil/suite/doc/15710506 . After the customer's RD is approved, the cell phone contract's contracting officer's representative (COR) or contracting officer's technical representative (COTR) will advise the GPC Holder identified in the RD how to log onto the contract site and order the cell phones. A detailed description of the ordering process is located at https://www.us.army.mil/suite/doc/15710662.

(b) Two-way wireless e-mail devices: All two-way wireless e-mail devices must be procured through the requirement document process. Requirement documents for two-way wireless e-mail devices must identify the following items: duty position that the device will be assigned to.

(c) Video teleconferencing (VTC) systems: All VTC systems must be procured from the AK VTC contract (https://www.us.army.mil/suite/doc/15711271) through the RD process. An example of a VTC RD is located at https://www.us.army.mil/suite/doc/15711068. A detailed description of the ordering process is located at https://www.us.army.mil/suite/doc/15711108.

(d) Servers: All servers be procured through the requirement document process and must be installed in the server farms in either Area II or Area IV.

(d) Non-standard office automation equipment: All non-standard office automation equipment must be procured through the requirement document process.

(e) The Area DOIM will forward all approved RDs for cell phones, two-way wireless e-mail devices, servers, and non-standard office automation equipment to the Regional DOIM for review and authorization.

(f) The Regional DOIM will forward all approved RDs for two-way wireless e-mail devices, servers, and non-standard office automation equipment to CESO-K for review and authorization. Cell phones are approved at this level. Additional Documentation.

(i) A Requirement Validation Document (RVD) must be submitted with each RD: https://www.us.army.mil/suite/doc/7157256.

(ii) Software. For items on the software Enterprise License Agreement (ELA), the appropriate Category-1, -2, or -3 Request Form must accompany the Requirement Document.
Cat-1 = https://www.us.army.mil/suite/doc/15734344
Cat-2 & Cat-3 = https://www.us.army.mil/suite/doc/7157249

(iii) Network Connectivity. This includes all network type devices (switches, routers, hubs etc.) A building diagram showing proposed locations for equipment and communications entry point must

accompany the RD. Also a network diagram and a risk management worksheet must be included in the RD packet. https://www.us.army.mil/suite/doc/15713254. For SIPR or RIPR requirements, an 8th US Army G-2 physical security assessment results memo, along with the unit commander/director's memo stating that unit will comply with G-2's memo, must be submitted.

(4) Land Mobile Radio (LMR). RD must be accompanied by:

(a) A memorandum from the Eighth Army Frequency Manager showing approved frequencies for the organization.

(b) A request for frequency assignment from the Eighth Army Frequency Manager in standard frequency action format (SFAF).

Paragraph 3-10, Information management/information technology human capital management. Insert the following sentence after the first sentence:

CESO-K is the proponent for Career Program CP34 in the Korean theater.

Paragraph 3-11, Registry for major information systems inventory, reduction, webification, and security. Add subparagraph h through i:

h. Eighth Army APMS Administrator will conduct the internal system data field review quarterly. All deficiencies will be notified to each system POC for immediate/corrective action.

i. Eighth Army APMS Administrator will provide APMS online training to new system POCs prior to grant permission to the real APMS server.

Paragraph 3-11b, Registry for major information systems inventory, reduction, webification, and security. Add subparagraph (3):

(3) Every system will maintain at least one primary and one alternate system POCs per system.

Paragraph 4-2, Compliance with Defense Information Systems Registry standards. Add the following: 1st Signal Brigade is responsible for developing and maintaining enterprise systems architectures for the AK. Eighth Army CIO/ACofS G6 is responsible for consolidating the systems architecture and operational architecture, and must conform to the current approved DOD Architecture Framework (DODAF) per DA Pamphlet 25-1-1, Para. 4.4 as it applies to AK. HQ Eighth Army staff offices, Eighth Army major subordinate commands (MSCs), and capability communities of interest (COIs) are responsible for developing and maintaining their own internal architecture product sets while informing and participating in AK architect-development teams.

Paragraph 5-4, Software Security. Add subparagraphs e through f.

e. Technical advice and assistance on the selection of software packages for security services is available from Eighth Army CIO/ACofS G6.

f. Software Accountability.

(1) Recordkeeping. The organization's Information Management Officer (IMO) must establish and maintain a recordkeeping system for software licenses, original media (optical, diskette or otherwise), user information. Consider the use of software management computer programs or locally developed databases,

spreadsheets, etc. to automate recordkeeping tasks.

(2) Storage. All original software licenses, original media (optical, diskette or otherwise), e-mail notification for approved software licenses, completed registration cards and other documentation should be stored in a locked and centralized location. The use of vendor-maintained web-based tracking systems is highly encouraged. For classified material storage, contact your security manager. Disposal of Software. Software is managed as a durable item. Although it does not require property book accountability, software will be controlled by the using organization's IMO. Excess commercial off-the-shelf (COTS) software should be disposed of according to normal property disposal procedures.

Paragraph 5-5, Hardware security. Add the following:
Technical advice and assistance on the selection of hardware-embedded security features is available from Eighth Army CIO/ACofS G6.

Paragraph 5-6, Procedural security. Add subparagraph e:

e. Upon receiving a report of a security incident from a user, the Information Assurance Security Officer (IASO) or Information Management Officer (IMO) will immediately report the incident to the Security Manager and Area DOIM Information Assurance Manager (IAM). If unable to contact the IAM, the IASO or IMO will attempt to contact the Regional Computer Emergency Response Team, Korea (RCERT-K). If still unsuccessful, the IASO or IMO will attempt to contact the Theater Network Operations and Security Center, Korea (TNOSC). Observe OPSEC when providing details to the incident.

Paragraph 5-8, Communications Security (COMSEC). Add the following:
Eighth Army CIO/ACofS G6 will prepare instructions and taskings for submitting COMSEC equipment requirements to HQDA CIO/ACofS G6 through the Information Systems Security Program (ISSP). Urgent requirements for COMSEC products must be supported by an operational needs statement according to AR 71-9. The Information Assurance Manager (IAM) will identify urgent requirements on the Information Systems Security Program (ISSP) web site at https://issp.army.mil.

Paragraph 6-1a, Information transmission economy and system discipline. Add subparagraphs (4) through (6):

(4) Telephone Control Officers (TCOs) request monthly DSN "99" use reports for their assigned organizations from their servicing dial central offices (DCOs) and maintain a detailed cell-phone usage report on all cell phones assigned in their area of responsibility.

(5) TCOs ensure all base communications (BASECOM) requirements above base-level services are validated in the service level agreements (SLAs) between their organizations and supporting signal battalions.

(6) Operators must use the long-distance service provider under contract to 1st Signal Brigade when placing calls to CONUS. When calling CONUS from the Korean theater, DSN operators may use commercial long-distance services for official calls that are not being made for command and control purposes. DSN operators will not transfer nonemergency morale calls to other operators for "off-netting" (transferring the call to a commercial line) if those calls result in fees being charged to the U.S. Government.

Paragraph 6-1i, Use of DOD-owned IT. Replace the second sentence with this paragraph:
Use of employee-owned IT personal electronic devices such as computers, hard drives, pocket drives, thumb drives, digital cameras, personal digital assistants (PDAs), etc., or software that connects to the network at the work site is prohibited. (See AR 25-2 "Information Assurance, paragraph 4-30"Employee-owned

Information Systems" for further guidance.) Use of Outlook Web Access (OWA) when combined with proper PKI-infrastructure, an SCR/CAC and appropriate network controls/access, from an employee-owned computer is authorized. A file may be transferred from employee-owned IT hardware to government-owned IT hardware only via e-mail, in which case government anti-virus software will check for malicious code before allowing the file to enter the network.

Paragraph 6-2c, DOD-provided processing services. Add subparagraph (4):

(4) Wireless information systems (ISs) are wireless telecommunications or computer-related equipment or interconnected systems or subsystems of equipment (including software, firmware, and hardware) used to support Army business, operations, and missions in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice or data. Wireless ISs include personal communications service (PCS) devices. Wireless ISs do not include one-way, receive-only devices. The use of Personal Area Network (PAN) technologies (i.e. Bluetooth, Zigbee and Ultra-wideband, etc.) are prohibited in the AK.

(a) Requests to implement a wireless connection to the LandWarNet (either Unclass or Class) must be sent to CESO-K for evaluation and approval. Each request must support an operational and mission need that cannot be met without the use of the wireless IS.

(b) Pilot and fielded wireless LANs and portable electronic devices (PEDs) with LAN connectivity must meet the same certification and accreditation (C&A) and information assurance (IA) requirements as wired LAN ISs.

(c) The "Wireless" security technical implementation guides (STIGs), which can be found at http://iase.disa.mil/stigs/index.html, will be used to help implement the security of DOD wireless information systems (ISs). Wireless devices and systems that do not meet the security requirements of the STIGs or of other appropriate DOD or Army policies will not be used to store, process, or transmit DOD information on AK networks unless approved by the Designated Approving Authority (DAA) as necessary to meet specific mission requirements. The "Wireless Security Checklist," available at http://iase.disa.mil/stigs/checklist/index.html, must be used to help confirm compliance with the requirements of the STIGs and other policies.

(d) Wireless ISs will not be configured to work with any device other than a Government-owned computer. When an approved device is used outside of the Army's infrastructure (e.g., during TDY, etc.), the device must be scanned for malicious codes before it can be reconnected to the AK backbone.

(e) Eighth Army CIO/ACofS G6 will certify that the device complies with spectrum supportability standards. All wireless devices must meet spectrum supportability and comply with Military Communications-Electronics Board (MCEB) standards, DOD Directive 5000.1, AR 5-12, and host-nation requirements. Because wireless devices do not require frequency assignments, the user will accept any interference received.

Paragraph 6-2d, Area Processing Centers (APC) and server consolidation. Add subparagraphs (3) through (5):

(3) Server Acquisition. AK organizations will not purchase servers without written approval from CESO-K. All servers will be installed in either the Area II or Area IV server farms.

(4) Server Connectivity and Accreditation.

(a) Before an organization connects a server to the AK network, the server must pass an "all audits" vulnerability scan and meet DISA STIG and IAVM requirements. The server hardware and software must be included in the Network Change Proposal (NCP) list for the circuit to which connected.

(b) No AK organization may activate an Exchange server without:

(i) Coordination with Eighth Army CIO/ACofS G6 and 1st Signal Brigade.

(ii) Approval from the Configuration Control Board (CCB).

(c) Organizations that have hardware systems not capable of operating in the Windows VISTA Enterprise environment must replace those systems or operate them in a stand-alone configuration, not connected to the Army in Korea (AK) network by 31 DEC 09. If an organization determines that a pre-Windows VISTA Enterprise operating system is required to perform its mission, it must submit a request for an exception to policy through CESO-K to HQDA, via the Asset & Vulnerability Tracking Resource (A&VTR) database (https://avtr.us.army.mil) that fully justifies why the old operating system must remain in use and the expected timeline to complete upgrading it to the current baseline operating system.

(5) Policy and Architectural Compliance. After a server is connected to the AK network, the Information Infrastructure Assessment Team will make periodic inspections to ensure that regulatory guidelines are followed. In addition, the Regional Computer Emergency Response Team, Korea (RCERT-K), will periodically conduct random network scans to verify server compliance.

Paragraph 6-2e(3), Enterprise software licenses. Add subparagraphs (d) through (f):

(d) The Army's software enterprise license agreement (ELA) was established to reduce the cost of software to the Army and to support Army Knowledge Management (AKM) goals by standardizing the desktop configuration, deploying Active Directory (AD) technology, and managing the Army's IT infrastructure.

(e) All Army in Korea (AK) units and organizations that have pre-existing agreements:

(i) May continue to use those agreements until they expire.

(ii) Are exempt from subparagraph (f) until that time.

(f) All Army in Korea (AK) units and organizations, except those covered by subparagraph (e), will:

(i) Follow ELA procedures for purchase of software and product services.

(ii) Fulfill the terms of any existing enterprise contracts before ordering software through the ELA.

(iii) Maintain accountability of software received through the ELA. Commanders must ensure distribution does not exceed the quantities authorized on the license certificate.

(iv) Allow only Information Management Officer (IMO) with valid appointment orders on file with the DOIM to request software. The appointment orders must be signed by the appointee's commander. If, for reasons of exercise or deployment, the commander is not physically present, an appointed representative may sign the appointment order.

(v) Order new or life-cycle replacement server hardware without operating system software. Workstations must be ordered with an operating system that includes only the NETCOM Enterprise Systems Technology Activity (ESTA) baseline. This requirement may be waived only by the CESO-K for legacy platforms that support defined requirements.

(vi) Use the ELA as their only source for services and software products covered by the ELA.

(vii) Use the Requirement Document process to procure services and software products covered by the software ELA. All requests are subject to the local DOIM's review.

Paragraph 6-2e(5), Software control. Add the following:
No software may be installed on AK networks without a valid Certificate of Networthiness (CoN) and written approval of the organizational Information Assurance Manager (IAM), CCB, and Designated Approving Authority(DAA). "AK networks" include LANs, departmental LANs, wireless-enabled portable electronic devices (PEDs), and standalone PCs. A copy of this approval must be kept with software records.

Paragraph 6-2k(1), Redistribution and disposal of IT Assets. Add the following:
Report all excess IT equipment to CESO-K for redistribution within the Korean theater. Do not turn the equipment in to the Defense Reutilization and Marketing Office (DRMO) without CESO-K's approval. For guidance on the procedures check AK PAM 25-1. Excess equipment listing can be found at: https://www.us.army.mil/suite/doc/4695963

Paragraph 6-3, Network Operations (NetOps). Add subparagraphs d through f.

d. Connection to Defense Information Systems Agency (DISA) Networks. In the Korean theater, the Theater Network Operations and Security Center, Korea (TNOSC-K) is responsible for regional oversight of local data networks that are connected to DISA networks.

LandWarNet(Unclas)=https://www.us.army.mil/suite/doc/7157254
RIPRNet = https://www.us.army.mil/suite/doc/7157257
LandWarNet (Clas) = https://www.us.army.mil/suite/doc/7157252

e. LAN Administration and Network Management. Supporting signal battalions are responsible for LAN administration and network management. To request installation of a LAN, the user will submit a RD to their Area DOIM. If the DOIM approves the request, he/she will determine the best method to design and install the LAN.

f. Remote Access. The Army in Korea (AK) remote-access request forms (categories 1 and 2) will be used by personnel in Korea to request remote access to the AK LandWarNet (Unclas) (See paragraph 3-7e2).

(1) The category 1 form will be used by DOD military personnel, DOD civilian employees, and permanently hired contractor personnel assigned to DOD agencies stationed in the Korean theater.

(2) The category 2 form will be used by contractor personnel who are temporarily hired to accomplish specific official tasks that require remote access to the network.

(3) The forms must be completed by the requesting user, the unit Information Management Officer (IMO), and the approving authority (either an O-5 or above commander, or GS-14 or above director).

(4) Commanders approving remote access for their personnel must provide correctly configured government-owned information systems (GOISs) for each user.

(5) The Contracting Officer Representative (COR) will also complete a portion of the category 2 form to validate that the requesting user is assigned to the contract and has an official requirement to remotely connect to the network.

(6) After the form has been completed and approved, the unit IMO will use it to complete an account request with the supporting signal battalion.

(7) These forms must be maintained in official files until the account is terminated or closed by the IMO in coordination with the supporting signal battalion. See AR 25-400-2 for further guidance.

(8) Employee-owned information systems (EOISs) are not authorized to be used to remotely connect to the AK LandWarNet (Unclas).

Paragraph 6-3c, Networthiness certification. Add subparagraphs (6) through (8):

(6) Networthiness applies to any network, system, and appliance, hereafter referred to as information system (IS) that requires accreditation under the Defense Information Technology Certification and Accreditation Process (DIACAP) and connects to, uses, manages, or is managed by the Army Enterprise Infostructure.

(a) Commercial-off-the-Shelf (COTS) software for which the Designated Approving Authority (DAA) requires an individual Defense Information Technology Certification and Accreditation Process (DIACAP) will also require individual Networthiness Certification. (If an upgrade to the software triggers an out-of-cycle re-accreditation, the Networthiness Certificate must also be updated.)

(b) COTS software that the Designated Approving Authority (DAA) accredits as part of a LAN or server DIACAP will not require the individual Networthiness Certification; the software is picked up from a Networthiness perspective as part of the higher-level accreditation. (If an upgrade to the software triggers an out-of-cycle re-accreditation for the LAN or server, the Networthiness Certificate must also be updated.)

(c) Information Management Officers (IMOs) should contact their DOIMs if assistance is required.

(d) Any IS operating without a Networthiness certificate is subject to removal from the Army in Korea (AK) enterprise network.

(7) CESO-K will:

(a) Provide Networthiness Certification Program oversight for AK.

(b) Assist AK IS functional and program management offices obtain Networthiness certification.

(c) Assist NETCOM in consolidating enterprise systems and operational architectures in the Korean theater.

(8) 1st Signal Brigade will:

(a) Serve as the Networthiness recommendation authority. Recommendations will be based on results of integrated logistics support, bandwidth, funding, and fielding analyses.

(b) Validate that the AK enterprise network can support ISs, that there are no negative effects to other ISs, that ISs do not introduce security vulnerabilities, and that ISs can be managed and maintained.

(c) Ensure that any IS operating on the AK enterprise network has an approved Networthiness certification.

(9) CESO-K Information Assurance Program Manager will:

(a) Validate the development of certification and accreditation (C&A) documentation by reviewing and endorsing such documentation and recommending action.

(b) Ensure ISs do not introduce security vulnerabilities.

(c) Make a Networthiness recommendation based on IA analysis.

(10) AK organization and activity commanders, heads of organizations assigned or attached to AK organizations, and AK IS functional managers will:

(a) Ensure ISs have a Networthiness certification before fielding.

(b) Request a Networthiness certification for AK-developed or -sponsored IS from NETCOM.

(c) All software must have a valid Certificate of Networthiness (CoN) before submitting an RD to purchase.

(i) CoN instructions: https://www.us.army.mil/suite/doc/15713308

(ii) CoN Check list for COTS and GOTS: https://www.us.army.mil/suite/doc/15713321

(iii) CoN Networthiness System Checklist: https://www.us.army.mil/suite/doc/15713322

Paragraph 6-4(4)b, Class B (Unofficial Telephone Service). Add the following:
Class B service is authorized on a reimbursable basis for quasi-governmental agencies, post exchanges, clubs and open/closed messes, other non-appropriated fund activities, private associations (including Boy Scout and Girl Scout activities), nursery activities, on-post concessionaires, and invited commercial contractors. Class B services will be charged IAW the Class B telephone rates that DISA publishes at the beginning of each fiscal year.

(a) Collect calls will not be accepted on class B phones.

(b) Service will provide local commercial access and Korea-wide DSN direct dial.

Eligible customers occupying on-post quarters on installations where Army & Air Force Exchange Service (AAFES) telephony service has been established by an approved AAFES commercial service provider may request personal telephone and broadband service only from the approved AAFES commercial service provider. Those housing areas and/or installations not serviced by the approved AAFES commercial service provider may contract services locally.

Paragraph 6-4g(4), Official telecommunications services in personal quarters of key personnel. Add the following:
A privately owned commercial cellular service may be used to satisfy the requirement for this separate service. Official DSN may not be used in the event of disruption or failure of commercial service. Commercial service must be maintained throughout the assignment and must be available for all members of the household. Failure to comply may result in punitive measures.

Paragraph 6-4m(3), Font style. Add the following:
At a minimum, the following communication types must be digitally signed: directions to subordinates; acknowledgement of or response to directions from superiors; financial information, to include committing, authorizing, or using government funds; contract information; statement of organization position/information to an external organization; email containing financial information (budgets, outlays, contract amounts); unclassified technical specifications or contract data; proprietary data; directives. In essence, email requiring data integrity, message authenticity, or non-repudiation of sensitive information shall be signed using DoD-approved PKI certificates. The addition of a digital signature increases the file size of an email message exponentially. Due to bandwidth restrictions, routine non-official emails should not contain digital signatures.

Paragraph 6-4m(5), Identification of POC and Office/Contractor status. Append to subparagraph (b):
This paragraph addresses specific issues affecting the Korea Region such as Korean Augmentees to the United States Army (KATUSAs) and foreign national (FN) employees. It also adds an Organization attribute to identify the lowest flagged unit the user is assigned to. Area DOIM offices and/or unit IMOs throughout the Korea Region will maintain all e-mail accounts using the display name policy depicted in Table 6-1 on page 20. **Table6-1. E-mail Display Names** Military Type = US Military, US Civilian, FN Civilian, Contractor, or KATUSA. Full Legal Name = Last, First, and Middle Names, and Generational ID (Jr., Sr., II, III). Do not use all caps. Do not use nicknames, call signs, or aliases. Title/Rank = Military Rank, or "CTR" for contractors. Use Mr., Ms., Miss, for civilians. Personal Type (PT) = MIL, CIV, CTR, RES (Mil Reserves), NG (National Guard), CG (Coast Guard), DoD Af (DoD Affiliates), DOD Ben (DoD Beneficiaries). Citizenship = three-letter ISO standard. KOR=Korean, USA DoD Component = USA, USN, USMC, or USAF. DoD Sub-Component = MACOM (NETCOM, MEDCOM, EUSA, USFK, etc.) Organization = Lowest Flagged Unit; often a battalion, not a company or detachment. Display Name = Name + Title/Rank + Personal Type + Citizenship + DoD Component + DoD Sub-Component + Organization. Use both upper and lower case. Use one comma after the last name. Do not use any periods.

Paragraph 6-4m(7). Use of encryption. Add subparagraph (e) and (f):

(e) CAC Replacement. Prior to replacing a CAC, the user should decrypt all stored, encrypted e-mails. Tools are available at the DOD public key encryption (PKE) Website: **https://www.us.army.mil/suite/page/474113**. The user must not decrypt e-mails by forwarding encrypted e-mail in unencrypted format to him/herself. In the event of an unplanned CAC replacement (i.e., lost a lost or stolen CAC), a copy of the user's old key may be obtained from the Automated Key Recovery Web site, https://ara-1.c3pki.chamb.disa.mil/ara/Key.

(f) CAC Personal Identification Number (PIN) Reset Procedures. In the event a user locks him/herself out of the CAC or forgets the PIN, he/she must reset it either at the CAC PIN Reset (CPR) Station located at the appropriate Area DOIM's office or at a CAC Issue Office.

Table 6-1. E-mail Display Names

Type	Last First MI Gen	Rank	PT	Cit	Comp	Sub-comp	Org	Display Name
US Military	Durham James R	PFC	MIL		USA	NETCOM	36 SIG BN	Durham, James R PFC MIL USA NETCOM 36 SIG BN
US Military	Marshall Andrew B	CPT	MIL		USA	MEDCOM	168 MED BN	Marshall, Andrew B CPT MIL USA MEDCOM 168 MED BN
US Military	Ray Bruce J	TSgt	MIL		USAF	USFK	USFK J6	Ray, Bruce J TSgt MIL USAF USFK J6
US Military	Bank Carl E	LCDR	MIL		USN	USFK	USFK J2	Bank, Carl E LCDR MIL USN USFK J2
US Military	Manning Kristine M	MAJ	MIL		USMC	USFK	USFK J64	Manning, Kristine M MAJ MIL USMC USFK J64
US Civilian	Hamilton Kenneth M III	Mr.	CIV		USA	NETCOM	1 SIG BDE	Hamilton, Kenneth M III Mr.CIV USA NETCOM 1 SIG BDE
US Civilian	Ortega Nancy A	Ms.	CIV		USA	IMCOM	IMCOM Korea	Ortega, Nancy A Ms.CIV USA IMCOM Korea
US Civilian	Spencer Robert A	Mr.	CIV		USA	ACA	CCK	Spencer, Robert A Mr. CIV USA ACA CCK
FN Civilian	Cho Nam Suk	Mr.	DoD Af	KOR	USA	IMCOM	IMCOM Korea	Cho, Nam Suk Mr.DoD Af KOR USA IMCOM Korea
FN Civilian	Kim Eun Hee	Ms.	DoD Af	KOR	USA	NETCOM	CESO-K	Kim, Eun Hee Ms.DoD Af KOR USA NETCOM CESO-K
Contractor	Leonard Steven R Jr	CTR	CIV		USA	EUSA	G3	Leonard, Steven R Jr CTR CIV USA EUSA G3
Contractor	Douglas Sandra D	CTR	CIV		USA	USFK	J3	Douglas, Sandra D CTR CIV USA USFK J3
KATUSA	Kim Suk Joon	SGM	DoD Af	KOR	USA	IMCOM	IMCOM Korea	Kim, Suk Joon SGM MIL KOR IMCOM Korea
KATUSA	Nam Min Yung	PV2	DoD Af	KOR	USA	INSCOM	501 MI BDE	Nam, Min Yung PV2 MIL KOR INSCOM 501 MI BDE

Paragraph 6-4m(11), E-mail administration . Add subparagraphs (g) through (i):

(g) Top level organizational unit (OU) administration and user account management are Area DOIM responsibilities. Those below the top level are OU Administrators. OU Administrators provide administration for the specific OU assigned. The OU Administrator performs all administrative functions within the site's OU. This includes the functions provided by the Help Desk Role as well as the ability to add and remove computers/servers, create and delete users and groups, move users to the In-transit OU, and change group membership within the OU.

(h) Personnel responsible for the management and maintenance of OU containers and objects within the OU will be delegated the rights and privileges to perform these tasks via a third-party tool. OU administrative roles and responsibilities include: user account management; print management; workstation management; data administration for member servers; group management; compliance with configuration management policies, architecture and naming standards; and creation of computer objects.

(i) The following e-mail practices are prohibited for all LandWarNet users: the use of stationery backgrounds; photos, clip art, or digital business cards in signature blocks. Official Web site URLs and official unit, corps, or regimental slogans/mottos are the only approved additions to the standard signature block (name, title, office, phone, and e-mail address).

Paragraph 6-4p, Video teleconferencing (VTC). Add subparagraphs (6) and (7):

(6) Eighth Army CIO/G6 is the approval authority for VTC systems and equipment. The 1st Signal Brigade operates and maintains VTC hubs in Korea and is responsible for developing and maintaining the VTC network architecture in Korea. The hubs provide multipoint VTC capability for secure command and control (C2) and common-user requirements. Certain VTC facilities are critical to the C2 of deployed forces. These facilities are directly connected to assigned ports on the secure VTC hub. Other VTC facilities will access the hub through commercial integrated services digital network (ISDN) dial-up for the duration of

scheduled VTCs.

(7) HQ Eighth Army staff principals and commanders of Eighth Army organizations and area support activities (ASAs) are responsible for:

(a) Operating and maintaining internal VTC systems.

(b) Registering H.320 and H.323 VTC systems with the Regional DOIM. Site registration forms and procedures are available in Appendix A of the "CONOPS for Republic of Korea VTC Hubs" at https://www.us.army.mil/suite/doc/15629933. Submit all registrations to the Regional DOIM.

(c) Configuring H.320 and H.323 VTC systems at an aggregate speed of 384 kbps.

(d) Obtaining, loading, and initiating appropriate COMSEC keys for secure VTC.

(e) Appointing a responsible and trained operator and alternate as POCs for VTC operations.

(f) Submitting an Army Knowledge Management (AKM) Goal 1 waiver request and RD for VTC systems and equipment that cost more than $25,000 dollars.

(g) Ensuring that a system accreditation package is submitted prior to connectivity being approved by the organizational Designating Approving Authority (DAA) in accordance with AR 25-2.

(h) Coordinating use of these common user VTC facilities through each unit's appropriate POCs.

(i) Understanding that the owner of a common user VTC facility may charge appropriately for any costs incurred for providing this service outside of normal operations.

Paragraph 6-4u(4), Local policies. Add the following:
Before a user is issued a government cell phone, the TCO must have the user read and sign the Army in Korea acceptable use policy (AUP) for cell phones, located at https://www.us.army.mil/suite/doc/12430208. The TCO must maintain soft or hard copies of all signed cell phone AUPs in records.

Paragraph 6-4y, Army management of electromagnetic spectrum. Add the following.
Refer to AR 71-9 "Material Requirements" for more information.

(1) All frequency use will be coordinated through the Eighth Army CIO/ACofS G6 Spectrum Manager, who will request frequencies from the Joint Frequency Management Office (JFMO). Units will not operate radio equipment in support of official business and missions without prior allocation of frequency spectrum by the Eighth Army CIO/ACofS G6 Spectrum Manager.

(2) Area Frequency Control Boards (AFCBs), consisting—at a minimum—of the Area Fire Chief, Area Provost Marshal, Area Medical Commander, and Installation Management Command Korea Region (IMCOM-K) Director or their designated representatives, will review all approved frequencies before implementation by units or activities. AFCBs are responsible for providing current fleet maps and currently used frequency lists to the Eighth Army CIO/ACofS G6 Frequency Manager and JFMO twice annually and for reviewing lists to determine frequencies and talk groups that are not in use. Frequencies not in use will be marked as such on fleet maps and frequency lists submitted to Eighth Army CIO/ACofS G6 and JFMO.

(3) Use of spectrum for satellite radios and phones must be approved by JFMO and the Eighth Army CIO/AcofS G6 Spectrum Manager. An operational needs statement (ONS) must be obtained from HQDA

before acquiring satellite equipment.

(4) Implementation guidance for spectrum management can be found at https://www.us.army.mil/suite/folder/363399.

Paragraph 6-4z, Radio Systems Support Services. Add subparagraphs (4) and (5).

(4) Purchase of all two-way radios for unit operations requires the approval of DOIM and must have—at a minimum—the following capabilities per United States Forces Korea (USFK) and U.S. Pacific Command (PACOM) policy letters:

(a) National Security Agency (NSA)-certified advanced encryption standard (AES) encryption

(b) Digital narrowband channelization (12.5 KHz), defined as the ability to stack radio channels with a spectrum distance between center frequencies at 12.5KHz. De-tuned wideband radios are strictly prohibited for future purchase. Acquisition managers seeking further information should contact CESO-K before purchasing commercial radios.

(c) Association of Public-safety Communications Officials (APCO)-25 compliance.

(d) Trunking Capability

(5) Operation of amateur radio within Korea requires a license from the Korean Ministry of Information and Communications (MIC). Amateur radio operators should apply for a license before operating radio equipment. Information can be found at http://www.karl.or.kr/. MIC generally requires 60-day processing time and an inspection of any equipment purchased outside Korea. The MIC's Web site is located at http://www.mic.go.kr/eng/index.jsp.

Paragraph 6-5, Long-Haul and Deployable Communications. Add subparagraph j:

j. Requesting Long-Haul Services. Units that need long-haul commercial services must submit a request for service (RFS). Refer to DA Pamphlet 25-1-1, para. 10-7 for RFS preparation instructions.

Paragraph 6-5a(2), Responsibilities. Add subparagraph (k):

(k) Network Remote Access. A "remote user" is a person who enters the AK LandWarNet (Unclas) from outside the physical or logical boundary of the internal LAN. The remote-access system creates a protected extension of the AK LandWarNet (Unclas) for authorized remote users.

(i) The LandWarNet (Unclas) remote-access system has the following components:

- Access to the network. Users will connect through the Terminal Server Access Control System (TSACS). TSACS provides unencrypted connection to the network.

- A Virtual Private Network (VPN). The primary function of VPN is to encrypt the path from the user to the network.

(ii) VPN will allow remote users to:

- Protect Army information that is sent and received during remote communications with other users and servers on the AK LandWarNet (Unclas).

- Use the applications available to them in their normal office environment.

(iii) Remote access to the AK LandWarNet (Unclas) will be used only for unclassified official business. Remote access will never be used to process classified data. Remote users will be subject to monitoring; their connection will be terminated if it causes damage to any part of the network or if their computer is not configured correctly. Personnel who abuse or misuse remote-access capabilities may have their remote-access account terminated and may be disciplined in accordance with the Uniform Code of Military Justice (UCMJ) or Office of Personnel Management (OPM) directives.

(iv) The 1st Signal Brigade will:

- Manage all remote-access points.

- Configure all remote-access equipment to require authentication and encryption. VPN functionality on remote-access equipment is required.

(v) Only an O-5 or above commander (or GS-14 or above director) may approve requests for remote access. These approval authorities will also be responsible for:

- Pre-approving reimbursement for TDY or remote-access connection charges at the user's home station.

- Setting specific limits when pre-approving reimbursement for connection charges. Generally, home-station remote-access users should not be reimbursed, because they normally can return to their office.

- Paying approved reimbursements for remote-access charges with internal operations and maintenance (O&M) funds.

(vi) Information Management Officers (IMOs) will:

- Use the appropriate AK remote-access request form to request approval for remote access with their supporting network service center (NSC).

- Keep completed forms (above) in unit records and coordinate new and deleted accounts with the supporting NSC per AR 25-400-2 "Army Records Information Management System (ARIMS)."

(vii) Employee-owned information systems (EOISs) are prohibited from connecting to the Army network for any purpose. If the approving authority determines that a person has a need for remote-access, then that authority must provide a GOIS. IMOs and remote-access users will complete AK Form 25-1K to ensure the GOIS to be used for remote access is correctly configured. .

Paragraph 6-7a(8), Web management policy**.** Add the following:
Each Army in Korea (AK) organization that manages a Web site will submit a Webmaster appointment memorandum through its respective DOIM to Eighth Army CIO/ACofS G6. The memorandum will specify a primary and alternate Webmaster and include an enclosed copy of his/her on-line Webmaster Training Course completion certificate. The on-line course is located at https://iatraining.us.army.mil. Each Webmaster will maintain a copy of his/her current Webmaster appointment memorandum and training certificate.

Paragraph 7-2f, Visual information Combat Camera (COMCAM). Add the following:
In Korea, COMCAM capabilities will be maintained by Eighth Army ACofS G3, in accordance with Operations Plan (OP) 50.27. The Korea Region Multimedia/Visual Information Support Center (MM/VISC) will maintain basic Combat Camera Capabilities to perform Combat Camera Duties until a Combat Camera team(s) from the 55th Combat Camera Company or the Joint Combat Camera Center can deploy into theater.

Paragraph 7-6, Equipment and systems. Add subparagraphs (i) and (j):

(i) Requests to purchase common-use VI equipment will be prepared using the Requirement Document (RD) process. DOIMs will coordinate with the Korea VI Regional Manager to obtain a validation memorandum authorizing procurement of the specified common-use VI equipment; otherwise, they will disapprove the RD.

(j) When possible, systems will be purchased/installed to meet the ergonomic requirements of users, consistent with the ergonomic requirements under applicable host-nation law. .

Paragraph 7-7a(6)(b)9. Multimedia/VI Productions. Add the following:
The Regional Visual Information (VI) Manager, will validate VI production requirements.

Paragraph 7-7a(6)(b)14a. Multimedia/VI Productions. Replace the first sentence with this sentence:
Requests for release of multimedia / visual information (VI) productions for loan or viewing by foreign military audiences will be forwarded to Regional VI Manager who will forward to Joint Visual Information Services Distribution Activity (JVISDA) for necessary administrative clearance.

Paragraph 7-7a(6)(b)14b. Multimedia / Visual Information (VI) Productions. Replace subparagraph b:

b. Requests for purchase of unclassified media by foreign civilian sources will be routed through the Regional Visual Information (VI) Manager who will route through Joint Visual Information Services Distribution Activity (JVISDA) to the US Army Security Assistance Command for clearance.

Paragraph 7-8g. Media library services. Add the following:
Media Library Services: The Korea Region Multimedia/Visual Information Support Center (MM/VISC) maintains an archive of Local AV Productions only. All other AV products may be ordered directly through the DefenseImagery.mil website.

Paragraph 8-2e(3), Management Concept. Insert the following sentence after the third sentence:
Within Eighth Army, the Assistant Chief of Staff ACofS G1 oversees records management policy.

Paragraph 8-5g, Freedom of Information Act program management. Add paragraphs (1) through (5):

(1) The Freedom of Information and Privacy Act Officer maintains a formal control system to track Freedom of Information Act (FOIA) case processing. All FOIA requests that organizations receive directly from requesters will be forwarded to: Commander, Eighth U.S. Army, (EAGA-PPR) (FOIA), Unit #15236, APO AP 96205-5236 for proper processing and to ensure accountability.

(2) Commanders/Directors/Chiefs of organizations will appoint in writing a Freedom of Information Act Official/Coordinator and a Privacy Act Official/Coordinator and submit a copy of the appointing document to: Commander, Eighth US Army, (EAGA-PPR) (FOIA), Unit #15236, APO AP 96205-5236.

(3) Freedom of Information Act (FOIA) Officials/Coordinators and Privacy Act (PA)

Officials/Coordinators, in addition to maintaining appropriate FOIA/PA directives, will become familiar with the provisions of these acts and prescribing directives. Additionally, persons appointed to these duties will schedule and complete training with the Freedom of Information and Privacy Act Officer within 60 days of their appointment. Training can be scheduled by calling 724-4549.

(4) The Freedom of Information and Privacy Act officer will provide Freedom of Information Act (FOIA) and Privacy Act (PA) briefings for organizations, on request, duty schedule permitting. Submit requests for training to: Commander, Eighth U.S. Army, (EAGA-PPR) (FOIA), Unit #15236, APO AP 96205-5236.

(5) The Freedom of Information and Privacy Act Officer maintains a formal control system to track Privacy Act (PA) case processing. All PA requests that organizations receive directly from requesters will be forwarded to: Commander, Eighth U.S. Army, (EAGA-PPR) (FOIA), Unit #15236, APO AP 96205-5236 for proper processing and to ensure accountability.

Paragraph 8-8, Army in Korea (AK) Records Management Policy. Add paragraph 8-8:

8-8. Army in Korea (AK) Records Management Policy

a. AR 25-400-2 provides basic records management policies and procedures. AK Pamphlet 25-68 prescribes responsibilities, policies, and procedures for transferring records (paper and digital) in the Korean theater.

b. AR 25-55 prescribes policies and procedures for managing records under the Freedom of Information Act.

c. AR 340-21 prescribes policies and procedures for managing records under the Privacy Act.

Chapter 9. Publications and Printing. Add paragraph 9-6:

9-6. Eighth Army in Korea. Within Eighth Army, the ACofS G1 oversees publications and printing policy.

Appendix A, Section I, Required Publications. Add the following items:

CJCSI 6740.01A, Military Telecommunications Agreements and Arrangements between the United States and Regional Defense Organizations or Friendly Foreign Nations DOD Directive 5000.1, The Defense Acquisition System DOD Directive 8100.2, Use of Commercial Wireless Devices, Services and Technologies in the DOD Global Information Grid (GIG)

Appendix A, Section II, Related Publications. Add the following items:
AR 79-1, Materiel Requirements AK Regulation 25-35, Preparing Army in Korea (AK) Publications

Glossary, Section I, Abbreviations. All abbreviations that appear in this supplement are listed either at the U.S. Army's Abbreviations, Brevity Codes, and Acronyms Web site (https://www.rmda.army.mil/abbreviation/MainMenu.asp) or in the AR 25-1 Glossary, except for the following:

A&VTR Asset & Vulnerability Tracking Resource

AD Active Directory

ADSL	Asymmetric Digital Subscriber Line
AFCB	Area Frequency Control Board
AK	Army in Korea
APCO	Association of Public-safety Communications Officials
CESO-K	Communications Enterprise Services Office—Korea
CPR	CAC PIN Reset
CTO	Certificate to Operate
DCO	Dial Central Office
EOIS	Employee-Owned Information System
ESTA	Enterprise Systems Technology Activity
FMS	Federal Information Processing Management System
GOIS	Government-Owned Information System
ICT	Information Communications Technology
IPv6	Internet Protocol, version 6
IS	Information System
JFMO	Joint Frequency Management Office
KTSC	Korea Theater Support Center
LMR	Land Mobile Radio
MIC	Ministry of Information and Communications
NSC	Network Service Center
ONS	Operational Needs Statement
OP	Operations Plan
OU	Organizational Unit
OWA	Outlook Web Access
PED	Portable Electronic Device
PKE	Public Key Encryption

PRWeb	Purchase Request Web
PSS	Preferred Subscriber Service
RCERT-K	Regional Computer Emergency Response Team, Korea
RVD	Requirement Validation Document
TNOSC-K	Theater Network Operations and Security Center, Korea
TSACS	Terminal Server Access Control System
TSAK	Training Support Activity Korea
UOC	Unit Operations Center US&P United States and Possessions
USACCK	United States Army Contracting Command, Korea
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network.